GOB Designs for Authentication Codes with Arbitration(Theory and Applications of Combinatorial Designs with Related Field)

AUTHOR(S):

Ge, Gennian; Miao, Ying; Zhu, L.

CITATION:

Ge, Gennian ...[et al]. GOB Designs for Authentication Codes with Arbitration(Theory and Applications of Combinatorial Designs with Related Field). 数理解析研究所講究録 2006, 1465: 24-38

ISSUE DATE:

2006-01

URL:

http://hdl.handle.net/2433/48032

数理解析研究所講究録 1465 巻 2006 年 24-38

GOB Designs for Authentication Codes with Arbitration

Gennian Ge
Department of Mathematics, Zhejiang University,
Hangzhou 310027, Zhejiang, P. R. China
E-mail: gnge@zju.edu.cn

Ying Miao
Department of Social Systems and Management,
Graduate School of Systems and Information Engineering,
University of Tsukuba, Tsukuba 305-8573, Japan
E-mail: miao@sk.tsukuba.ac.jp

L. Zhu
Department of Mathematics, Suzhou University,
Suzhou 215006, P. R. China
E-mail: lzhu@suda.edu.cn

Abstract

Combinatorial characterization of optimal authentication codes with arbitration was previously given by several groups of researchers in terms of affine α-resolvable + BIBDs and α-resolvable designs with some special properties, respectively. In this paper, we revisit this known characterization and restate it using a new idea of GOB designs. This newly introduced combinatorial structure simplifies the characterization, and enables us to extend Johansson's well-known family of optimal authentication codes with arbitration to any finite projective spaces with dimension greater than or equal to 3.

1 Introduction

Authentication codes (A-codes) were invented in 1974 by Gilbert, MacWilliams and Sloane [2] for protecting the integrity of information. These codes involve three active parties: a *transmitter* T, a *receiver* R, and an *opponent* O. The transmitter T transmits messages to the receiver R using a communication channel. The opponent O has access to the channel, and can interfere with the contents of cryptograms transmitted via this channel. Two different types of attacks from the opponent O, *impersonation* and *substitution* attacks, are usually considered. A game-theoretic model for authentication codes was developed in 1982 by Simmons [13]. Many other people also contributed to the theory of authentication codes, see, for example, [6, 3, 16, 12].

However, the above model is restricted. In this conventional A-code, T and R use the same key, and thus they should trust each other, which is not always the case in reality.

It is quite possible that T sent a message and then later denies having sent it or, on the other hand, R claims to have received a message that was never sent by T.

Simmons [14, 15] then introduced an extended authentication model called *authentication codes with arbitration*, or simply A^2-codes, to provide protection against deceptions from T and R as well as that from O. This model for A^2-codes includes a fourth party, the *arbiter* A, who arbitrates if T or R cheats. The arbiter A does not take part in any communication activities on the channel. By definition, A has access to all key information and does not cheat.

For this model of A^2-codes, Johansson [4] derived entropy based lower bounds on the cheating probabilities and the sizes of keys, which were later generalized to A^2-codes protecting *spoofing* of high order by Wang, Safavi-Naini and Pei [18]. Kurosawa and Obana [5] showed combinatorial lower bounds on them. Obana and Kurosawa [8] characterized optimal A^2-codes, that is, A^2-codes with the minimum cheating probabilities and the minimum sizes of keys, in terms of affine α-resolvable + BIBDs. Wang, Safavi-Naini and Pei [18] characterized ℓ-optimal A^2-codes, which offer the best protection for spoofing of order up to ℓ and require the minimum sizes of keys, in terms of α-resolvable and strong partially balanced resolvable designs. Similar results can also be found in, for example, [7, 17, 10, 9]

Very little is known about the construction of optimal A^2-codes. Some references related to this problem include [14], [15] and [4]. Combinatorial characterization of optimal A^2-codes can reduce the construction of optimal A^2-codes to the construction of their corresponding combinatorial structures. Unfortunately, both affine α-resolvable + BIBDs and α-resolvable and strong partially balanced resolvable designs are too complicated to be used effectively to construct optimal A^2-codes. In this paper, we introduce a new concept of GOB designs. Although this new combinatorial structure is essentially the same as those mentioned above, it does make the characterization more clear, and does enable us to construct new optimal A^2-codes. Johansson [4] constructed a well-known family of optimal A^2-codes in projective spaces $\mathrm{PG}(3, q)$. This is in fact a family of GOB designs, and we will extend this family to $\mathrm{PG}(n, q)$ for $n \geq 3$ in Section 5, which gives a new family of optimal A^2-codes containing Johansson's as a special case.

2 Authentication Codes with Arbitration

Contrary to a conventional A-code, an A^2-code is an *asymmetric* authentication system defined by the following two sets of cryptographic functions: a set of *encoding functions* used by the transmitter T to generate *authenticated messages*, and a set of *verification functions* used by the receiver R to verify authenticity of received messages. We assume a probability distribution $p_S(s)$ on the set S of source states and a probability distribution $p_{E_T \times E_R}(e_T, e_R)$ on $E_T \times E_R$ respectively, where E_T is the set of T's keys and E_R the set of R's keys. Given these probability distributions, it is straightforward to compute the probability distributions $p_{E_T}(e_T)$ and $p_{E_R}(e_R)$ on E_T and E_R respectively. The set of encoding functions is indexed by T's key, $e_T \in E_T$, while the set of verification functions

is indexed by R's key, $e_R \in E_R$. T uses his *secret key*, $e_T \in E_T$, to determine an *encoding function* f to encode a *source state* $s \in S$, and then sends the *authenticated message* $m \in M$ to R,

$$f : E_T \times S \longrightarrow M.$$

R uses his *secret key*, $e_R \in E_R$, to determine a *verification function* g to verify authenticity of the received message,

$$g : E_R \times M \longrightarrow S \cup \{\text{reject}\}.$$

Decoding may result in acceptance of the message as a particular source state, or rejection of it and declaring it fraudulent. Let $E_T \circ E_R = \{(e_T, e_R) \in E_T \times E_R :$ if $f(e_T, s) = m$ and $p_{E_T \times E_R}(e_T, e_R) > 0$, then $g(e_R, m) = s$ for all $s \in S\}$. The keys for T and R are chosen from $E_T \circ E_R$ according to a certain probability distribution over $E_T \circ E_R$. In fact, key generation for this asymmetric authentication system can be coordinated by the arbiter A in several ways (see, for example, [4, 18]). In all cases A will end up by knowing the keys of both T and R, and therefore in this model, we have to assume that A is trusted by both T and R. We denote an A^2-code by $(\mathcal{S}, \mathcal{M}, \mathcal{E}_T, \mathcal{E}_R)$, where for any set X, $\mathcal{X}$ denotes a random variable over X.

In an A^2-code, three types of attacks have been considered and lower bounds on the success probabilities of attacks have been derived in each case.

- **Attacks from the opponent O**

  Attack I: Impersonation by O. O sends a message m to R. O succeeds if m is accepted by R as authentic.

  Attack S: Substitution by O. O observes a message m, and substitutes m with another message $m' \neq m$, then sends m' to R. O succeeds if m' is accepted by R as authentic, and m, m' represent distinct source states.

- **Attack from the transmitter T**

  Attack T: Impersonation by T. T sends a message m to R and then denies having sent it. T succeeds if m is accepted by R as authentic and $m \neq f(e_T, s)$ for any $s \in S$.

- **Attacks from the receiver R**

  Attack R_0: Impersponation by R. R claims to have received a message m from T. R succeeds if T can generate m.

  Attack R_1: Substitution by R. R receives a message m from T but claims to have received another message m' such that $s' \neq s$, where $f^{-1}(m') = (e_T, s')$ and $f^{-1}(m) = (e_T, s)$. R succeeds if T can generate m'.

In all the possible attempts to cheat it is understood that the cheating party uses an optimal strategy when choosing a message or, equivalently, that the cheating party chooses the message that maximizes his chance of success. For the possible deceptions mentioned above, we denote the probabilities of success in each attack by P_I, P_S, P_T, P_{R_0}, and P_{R_1}, respectively.

In an A^2-code, let $\mathcal{M}^i$ denotes the random variable for the first i messages sent by T, $\mathcal{M}^c$ the random variable for messages that are not valid under the given encoding functions, and $H(\mathcal{Z}|\mathcal{X})$ the conditional entropy. Johansson [4] derived lower bounds on the cheating probabilities and the sizes of keys as follows.

Proposition 2.1 [4] Then the following inequalities hold:

$$\begin{aligned}
P_I &\geq 2^{H(\mathcal{E}_R|\mathcal{M})-H(\mathcal{E}_R)}, \\
P_S &\geq 2^{H(\mathcal{E}_R|\mathcal{M}^2)-H(\mathcal{E}_R|\mathcal{M})}, \\
P_T &\geq 2^{H(\mathcal{E}_R|\mathcal{M}^c,\mathcal{E}_T)-H(\mathcal{E}_R|\mathcal{E}_T)}, \\
P_{R_0} &\geq 2^{H(\mathcal{E}_T|\mathcal{M},\mathcal{E}_R)-H(\mathcal{E}_T|\mathcal{E}_R)}, \\
P_{R_1} &\geq 2^{H(\mathcal{E}_T|\mathcal{M}^2,\mathcal{E}_R)-H(\mathcal{E}_T|\mathcal{M},\mathcal{E}_R)}, \\
|E_R| &\geq (P_I P_S P_T)^{-1}, \\
|E_T| &\geq (P_I P_S P_{R_0} P_{R_1})^{-1}, \\
|E_T \circ E_R| &\geq (P_I P_S P_T P_{R_0} P_{R_1})^{-1}.
\end{aligned}$$

In a Cartesian A-code, the authenticated message $m \in M$ corresponding to a source state $s \in S$ encoded using $e_T \in E_T$ is the concatenation $m = (s, a)$ of the source state $s \in S$ and an authentication tag $a \in AT$, that is, $M = S \times AT$, where AT is the set of authentication tags. The receiver R will detect a fraudulent message $(s, a) \in M$ if his verification $g(e_R, (s, a)) =$ rejection or $g(e_R, (s, a)) \neq s$. For a verification function g determined by $e_R \in E_R$ and for $s \in S$, let

$$Split(g, s) = \{(s, a) \in M : g(e_R, (s, a)) = s\}.$$

A Cartesian A^2-code is said to be an (ℓ, c) A^2-code if $|M|/|S| = |AT| = \ell$, and $|Split(g, s)| = c$ for all verification functions g determined by all $e_R \in E_R$ and for all $s \in S$.

Kurosawa and Obana [5] showed combinatorial lower bounds on the cheating probabilities as follows.

Proposition 2.2 [5] In an (ℓ, c) A^2-code,

1. $P_I \geq c/\ell$. The equality holds if and only if $Pr[R \text{ accepts } m] = c/\ell$ for all $m \in M$.
2. If $P_I = c/\ell$, then $P_S \geq c/\ell$. The equality holds if and only if $Pr[R \text{ accepts } (s', a') \mid T \text{ sent } (s, a)] = c/\ell$ for all $(s, a), (s', a') \in M$ such that $s \neq s'$.
3. $P_T \geq (c-1)/(\ell-1)$. The equality holds if and only if $Pr[R \text{ accepts } m \mid T \text{ has } e_T] = (c-1)/(\ell-1)$ for all $e_T \in E_T$ and for all $m \notin M(e_T)$, where $M(e_T) = \{m \in M : m = f(e_T, s) \text{ for some } s \in S\}$.
4. $P_{R_0} \geq 1/c$. The equality holds if and only if $Pr[T \text{ can generate } (s, a) \mid R \text{ has } e_R] = 1/c$ for all $e_R \in E_R$ and for all $(s, a) \in M(e_R)$, where $M(e_R) = \{(s, a) \in M : g(e_R, (s, a)) = s\}$.

5. If $P_{R_0} = 1/c$, then $P_{R_1} \geq 1/c$. The equality holds if and only if $Pr[T$ can generate (s, a) and $(s', a') \mid R$ has $e_R] = 1/c^2$ for all $e_R \in E_R$ and for all $(s, a), (s', a') \in M(e_R)$ such that $s \neq s'$.

From Propositions 2.1 and 2.2, we can easily obtain the following combinatorial lower bounds on the sizes of keys.

Corollary 2.3 If all the equalities of Proposition 2.2 are satisfied, then

$$|E_T| \geq \ell^2, \ |E_R| \geq \frac{\ell^2(\ell-1)}{c^2(c-1)}, \ |E_T \circ E_R| \geq \frac{\ell^2(\ell-1)}{(c-1)}.$$

Corollary 2.4 [5] If all the equalities of Proposition 2.2 and Corollary 2.3 are satisfied, then $|S| \leq c + 1$.

An (ℓ, c) A^2-code is said to be *optimal with respect to cheating probabilities* if all the bounds of Proposition 2.2 are met. An (ℓ, c) A^2-code is said to be *optimal with respect to cheating probabilities and key sizes* if it is optimal with respect to cheating probabilities and the bounds of Corollary 2.3 are met. An (ℓ, c) A^2-code is said to be *optimum* if it is optimal with respect to cheating probabilities and key sizes and the bound in Corollary 2.4 is met.

3 GOB Designs

Given a set $\mathcal{V}$ of v elements $s_1, s_2, \ldots, s_v$, a relation satisfying the following conditions is said to be an *association scheme* with m classes.

1. Any two elements are either 1st, 2nd, ..., or mth associates, the relation of association being symmetric; that is, if the element α is the ith associate of the element β, then β is the ith associate of α.

2. Each element α has n_i ith associates, the number n_i being indepedent of α.

3. If any two elements α and β are ith associates, then the number of elements that are jth associates of α, and kth associates of β, is p^i_{jk} and is independent of the pair of ith associates α and β.

The numbers v, n_i $(i = 1, 2, \ldots, m)$ and p^i_{jk} $(i, j, k = 1, 2, \ldots, m)$ are called the *parameters* of the association scheme.

If we have an association scheme with m classes and given parameters, we obtain a *partially balanced incomplete block design*, or simply *PBIB design*, with m associate classes if the v elements of $\mathcal{V}$ are arranged into b subsets called *blocks* of size k $(< v)$ such that

1. every element occurs at most once in a block;
2. every element occurs in exactly r blocks;
3. if two elements α and β are ith associates, then they occur together in λ_i blocks, the number λ_i being independent of the particular pair of ith associates α and β.

The numbers v, b, r, k, λ_i $(i = 1, 2, \ldots, m)$ are called the *parameters* of the PBIB design.

A PBIB design with two associate classes is said to be *group divisible*, or simply *GD*, if there are $v = mn$ elements and the elements can be divided into m groups of n elements each, such that any two elements of the same group are first associates and any two elements from different groups are second associates.

A GD design with $k = m$, $\lambda_1 = 0$ and $\lambda_2 = \lambda$ is usually called a *transversal design*, denoted by $\mathrm{TD}_\lambda(m, n)$. If λ is omitted in the notation it is understood to be 1.

Balanced incomplete block designs, or simply *BIB designs*, are degenerated cases of PBIB designs in which $\lambda_1 = \lambda_2 = \cdots = \lambda_m = \lambda$. This means that for defining BIB designs, we in fact do not need the concept of association schemes. More precisely, a BIB design is an arrangement of the v elements of $\mathcal{V}$ into b subsets called *blocks* each of size k $(< v)$ satisfying the following conditions.

1. Every element occurs at most once in each block.
2. Every element occurs in exactly r blocks.
3. Every pair of distinct elements occurs together in λ blocks.

Suppose that $\mathcal{V}$ is a set of points, $\mathcal{U} \subseteq \mathcal{V}$, and $\mathcal{B}$ is a collection of subsets (or blocks) of $\mathcal{V}$. We call $\mathcal{B}_\mathcal{U} = \{B \cap \mathcal{U} : B \in \mathcal{B}\}$ the *restriction* of $\mathcal{B}$ to $\mathcal{U}$.

A combinatorial structure closely related to a transversal design is an orthogonal array. An *orthogonal array* $\mathrm{OA}_\lambda(k, n)$ is a $\lambda n^2 \times k$ array of n symbols such that, in any two columns of the array, every one of the possible n^2 pairs of symbols occurs in exactly λ rows. If λ is omitted in the notation it is understood to be 1. It is well known that an $\mathrm{OA}_\lambda(k, n)$ is equivalent to a $\mathrm{TD}_\lambda(k, n)$.

Now we introduce the notion of a GOB design. Let $\mathcal{V}$ be a set of $t\ell$ elements, and $\mathcal{G}$ a partition of $\mathcal{V}$ into t *groups* of ℓ elements each such that any two elements in the same group are 1st associates and any two elements from different groups are 2nd associates. A (t, ℓ, c, λ)-*GOB design* $(\mathcal{V}, \mathcal{G}, \mathcal{B})$ is a GD design with $\lambda_1 = q_1$ and $\lambda_2 = q_2$ such that

1. any block in $\mathcal{B}$ is of size tc containing exactly c elements from each of the t groups in $\mathcal{G}$;
2. for any distinct groups $G_i, G_j, G_k \in \mathcal{G}$ and any fixed elements $x, y \in \mathcal{V}$ with $x \in G_i$ and $y \in G_j$, there exists a point $z \in G_k$ such that z belongs to all the blocks containing both x and y;

3. for any fixed group $G \in \mathcal{G}$ and any fixed element $x \notin G$, the restriction of the blocks containing x to G forms an (ℓ, c, λ)-BIBD.

If we interchange the roles of elements and blocks in the definition of a GOB design, we obtain an affine c-resolvable + BIB design introduced in [8] and α-resolvable designs with special properties in [10, 18]. Affine c-resolvable + BIB designs were proved in [8] to be equivalent to optimal (ℓ, c) A^2-codes. α-Resolvable designs with special properties were also used in [10, 18] to characterize optimal A^2-codes. Although the concept of a GOB design and those of an affine c-resolvable + BIB design and an α-resolvable design with special properties are essentially the same, we prefer the terminology of GOB designs than those of affine c-resolvable + BIB designs and α-resolvable designs, because we deem that the concept of a GOB design is easier to be described and understood, and thus it may lead us to new constructions for optimal A^2-codes. It turns out that our expectation can be fulfilled.

In the above definition the parameters $t, \ell, c, q_1, q_2, \lambda$ are mentioned. Let b be the number of all blocks in $\mathcal{B}$ and r be the number of all blocks in $\mathcal{B}$ containing any fixed element. Similarly to Lemma 5 in [8], we can deduce the relations among these parameters from the present definition.

By the definition of a GOB design, the restriction of all blocks to any group $G \in \mathcal{G}$ is an (ℓ, c, q_1)-BIB design. This gives

$$b = q_1 \frac{\ell(\ell-1)}{c(c-1)} \tag{3.1}$$

and

$$r = q_1 \frac{\ell - 1}{c - 1}. \tag{3.2}$$

From the (ℓ, c, λ)-BIB design in condition (3) of the definition for a GOB design, we have

$$r = \lambda \frac{\ell(\ell-1)}{c(c-1)} \tag{3.3}$$

and

$$r^* = \lambda \frac{\ell - 1}{c - 1}, \tag{3.4}$$

where r^* is the number of blocks containing a fixed element in the restricted (ℓ, c, λ)-BIB design.

Suppose that the (ℓ, c, λ)-BIB design is obtained by fixing a group $G \in \mathcal{G}$ and an element $x \notin G$. Suppose also that the fixed element in the (ℓ, c, λ)-BIB design is $y \in G$. Then the number of blocks containing $y \in G$ in the (ℓ, c, λ)-BIB design is the same as the number of blocks containing both $x \notin G$ and $y \in G$. That is,

$$r^* = q_2. \tag{3.5}$$

From equations (3.2) and (3.3), we obtain

$$q_1 = \lambda\frac{\ell}{c}. \tag{3.6}$$

Combining equations (3.1) and (3.6), we obtain

$$b = \lambda\frac{\ell^2(\ell-1)}{c^2(c-1)}. \tag{3.7}$$

Summarily, the following relations always hold among parameters of a GOB design.

Proposition 3.1 In a (t, ℓ, c, λ)-GOB design,

$$v = t\ell,\ b = \lambda\frac{\ell^2(\ell-1)}{c^2(c-1)}, r = \lambda\frac{\ell(\ell-1)}{c(c-1)}, k = tc, q_1 = \lambda\frac{\ell}{c},\ q_2 = \lambda\frac{\ell-1}{c-1}.$$

We can also derive a lower bound for the parameter t from Rao's bound [11] for an orthogonal array.

In fact, condition (2) of the definition for a GOB design $(\mathcal{V}, \mathcal{G}, \mathcal{B})$ implies that there exists an $\mathrm{OA}(t, \ell)$. Equivalently, we show that there exists a $\mathrm{TD}(t, \ell)$ with $\mathcal{G} = \{G_1, G_2, \ldots, G_t\}$ as its groups. For any two elements x, y from distinct groups G_i and G_j, by the fact that a GOB design is also a GD design, we have exactly λ_2 blocks $B_1, B_2, \ldots, B_{\lambda_2} \in \mathcal{B}$ containing both x and y. Denote their intersection by $T(x, y)$. By condition (2), for any third group G_k there is an element $z \in G_k$ such that $z \in T(x, y)$. Since $T(x, y)$ intersects each group, we have $|T(x, y)| \geq t$. On the other hand, we can show that $|T(x, y)| \leq t$ and thus $|T(x, y)| = t$. Otherwise, $T(x, y)$ intersects some group $G \in \mathcal{G}$ in two elements w_1 and w_2. Since $B_1, B_2, \ldots, B_{\lambda_2}$ all contain both w_1 and w_2, we get $\lambda_2 \leq \lambda_1$. This contradicts to Lemma 3.1. Denote

$$\mathcal{A} = \{T(x, y) : x \in G_1, y \in G_2\}.$$

Then $\mathcal{A}$ is the block set of the desired $\mathrm{TD}(t, \ell)$. We need to show that any two blocks A_1, A_2 in $\mathcal{A}$ can not have two common elements. If not so, then A_1 and A_2 have two common elements z and w from distinct groups. This forces $A_1 = T(z, w) = A_2$, a contradiction.

Proposition 3.2 If there exists a (t, ℓ, c, λ)-GOB design, then there exists an $\mathrm{OA}(t, \ell)$.

Rao's bound [11] claims that in an $\mathrm{OA}_\lambda(k, n)$, the inequality

$$\lambda n^2 \geq k(n-1) + 1$$

always holds. So we have

$$\ell^2 \geq t(\ell-1) + 1.$$

This gives the following necessary condition on parameters.

Corollary 3.3 If there is a (t, ℓ, c, λ)-GOB design, then $t \leq \ell + 1$.

We finally remark that the newly introduced (t, ℓ, c, λ)-GOB design is named after its three intrinsic combinatorial structures, that is, a **GD** design, an $\mathbf{OA}(t, \ell)$, and an (ℓ, c, λ)-**BIBD**.

4 The Known Equivalence Revisited

Obana and Kurosawa [8] proved that optimal A^2-codes are equivalent to affine α-resolvable + BIBDs. Li, Pei, Safavi-Naini and Wang [10, 18] also proved the equivalence in terms of α-resolvable designs with special properties. In this section, we revisit this equivalence from a design-theoretic point of view. This enables us to simplify the original proofs and make things more clear.

Suppose that there exists an optimal Cartesian (ℓ, c) A^2-code $(\mathcal{S}, \mathcal{M}, \mathcal{E}_T, \mathcal{E}_R)$. For each source state $s \in S$, define a group $G_s = \{s\} \times AT \in \mathcal{G}$, where AT is the set of all possible authentication tags. Then we obtain $|S|$ groups. Since $(\mathcal{S}, \mathcal{M}, \mathcal{E}_T, \mathcal{E}_R)$ is an optimal (ℓ, c) A^2-code, $M = S \times AT$, $|AT| = \ell$, and $|G_s| = \ell$ for any group $G_s \in \mathcal{G}$.

Each $e_T \in E_T$ can be considered as a mapping from the set S of source states to the set AT of authentication tags, and each $e_T \in E_T$ can be expressed as the $|S|$-subset $\{(s, e_T(s)) : s \in S\}$. Similarly, each $e_R \in E_R$ can be considered as a mapping from the set M of the messages to the set $\{0, 1\}$, where for the verification function g determined by e_R

$$g : E_R \times M \longrightarrow S \cup \{\text{reject}\},$$

if $g(e_R, (s, a)) = s$ then $e_R(s, a) = 1$, otherwise $e_R(s, a) = 0$, and e_R can be expressed as the set $\cup_{s \in S} Split(g, s)$ by defining $(s, a) \in e_R$ if and only if $e_R(s, a) = 1$. Then from the definition of $Split(g, s)$, e_R has c common elements with each group $G_s \in \mathcal{G}$ and $|e_R| = c|S|$.

We first prove that the associated $(M, \mathcal{G}, E_T)$ forms a TD$(|S|, \ell)$.

Theorem 4.1 $(M, \mathcal{G}, E_T)$ is a TD$(|S|, \ell)$.

Proof: For any two elements $(s, a), (s', a') \in M$ from distinct groups, by the optimality of the (c, ℓ) A^2-code, we know that $Pr[(s', a') \in e_R \mid (s, a) \in e_T] = c/\ell > 0$ provided that $(e_T, e_R) \in E_T \circ E_R$. Since R accepts whatever T honestly sends, e_T contains both (s, a) and (s', a'). Therefore there are at least ℓ^2 such e_T's. However $|E_T| = \ell^2$. This means that the above e_T is the unique block containing (s, a) and (s', a'), which implies that $(M, \mathcal{G}, E_T)$ is a TD$(|S|, \ell)$. □

Now we prove that the associated $(M, \mathcal{G}, E_R)$ forms a GOB.

Theorem 4.2 The associated $(M, \mathcal{G}, E_R)$ forms an $(|S|, \ell, c, 1)$-GOB design.

Proof: We already knew that property (1) required in the definition of a GOB design is satisfied, that is, e_R has c common elements with each group $G \in \mathcal{G}$ and $|e_R| = c|S|$.

We prove property (3), that is, for all $(s, a), (s', a'), (s', a'') \in M$ with $s \neq s'$ and $a' \neq a''$, there exists exactly one $e_R \in E_R$ containing $(s', a'), (s', a'')$. From Theorem 4.1, there exists an $e_T \in E_T$ containing (s, a) and (s', a'). Suppose $(e_T, e_R) \in E_T \circ E_R$. Then $(s, a), (s', a') \in e_R$, and by the optimality of the (c, ℓ) A^2-code, $Pr[(s', a'') \in e_R \mid \mathcal{E}_T =$

$e_T] = (c-1)/(\ell-1) > 0$, which implies that $(s, a'') \in e_R$. So altogether there are at least $\ell \times (\ell \times (\ell-1))$ such e_R's. However, since $|e_R \cap G| = c$ for any group $G \in \mathcal{G}$, every block e_R is repeatedly counted $c \times (c \times (c-1))$ times. This means that altogether there are at least $\frac{\ell^2(\ell-1)}{c^2(c-1)}$ e_R's, not counting multiplicities. But the optimality tells us that $|E_R| = \frac{\ell^2(\ell-1)}{c^2(c-1)}$. This means that the block $e_R \in E_R$ containing $(s, a), (s', a'), (s', a'') \in M$ is unique.

Now we prove $(M, \mathcal{G}, E_R)$ is a GD design with $\lambda_1 = (\ell-1)/(c-1)$ and $\lambda_2 = \ell/c$, that is, for all $(s, a), (s', a'), (s', a'') \in M$ with $s \neq s'$ and $a' \neq a''$, there exist exactly $(\ell-1)/(c-1)$ and ℓ/c blocks $e_R \in E_R$ containing $(s, a), (s', a')$ and $(s', a'), (s', a'')$, respectively. For all $a'' \in AT$ with $a' \neq a''$, there exists exactly one block $e_R \in E_R$ containing $(s, a), (s', a'), (s', a'')$. Therefore there are exactly $\ell - 1$ blocks, counting multiplicities, containing $(s, a), (s', a')$. Every block intersects the group $\{s'\} \times AT$ at $c-1$ elements other than (s', a'). Then we know that there are exactly $(\ell-1)/(c-1)$ blocks, not counting multiplicities, containing $(s, a), (s', a')$. Similarly, for all $(s, a) \in \{s\} \times AT$ with $s \neq s'$, there exists exactly one block $e_R \in E_R$ containing $(s, a), (s', a'), (s', a'')$. Therefore there are exactly ℓ blocks, counting multiplicities, containing $(s', a'), (s', a'')$. Every block intersects the group $\{s\} \times AT$ at c elements, and consequently, there are exactly ℓ/c blocks, not counting multiplicities, containing $(s', a'), (s', a'')$.

Finally we prove property (2), that is, for all $(s, a) \in \{s\} \times AT$, $(s', a') \in \{s'\} \times AT$ with $s \neq s'$, and $s'' \in S \setminus \{s, s'\}$, there exists an element $(s'', a'') \in \{s''\} \times AT$ belonging to all the blocks containing $(s, a), (s', a')$. Suppose $(s, a), (s', a') \in e_T$. Then there exist exactly $(\ell-1)/(c-1)$ blocks $e_R \in E_R$ containing $(s, a), (s', a')$. Therefore, $|\{e_R \in E_R : (e_T, e_R) \in E_T \circ E_R\}| \leq (\ell-1)/(c-1)$. If $|\{e_R \in E_R : (e_T, e_R) \in E_T \circ E_R\}| < (\ell-1)/(c-1)$, then there would exist a block e'_R such that $(e_T, e'_R) \in E_T \circ E_R$ and $Pr(\mathcal{E}_\mathcal{R} = e'_R \mid \mathcal{E}_T = e_T) > (c-1)/(\ell-1)$. This implies that $P_T > (c-1)/(\ell-1)$ which is a contradiction to the optimality. So we know that $|\{e_R : (e_T, e_R) \in E_T \circ E_R\}| = (\ell-1)/(c-1)$. This means that all the $(\ell-1)/(c-1)$ blocks containing $(s, a), (s', a')$ contain also $(s'', e_T(s''))$ for all $s'' \in S \setminus \{s, s'\}$.

The proof is then completed. □

Conversely, from a GOB design, we can also construct an optimal Cartesian A^2-code.

Theorem 4.3 If there exists a $(t, \ell, c, 1)$-GOB design $(\mathcal{V}, \mathcal{G}, \mathcal{B})$, then there exists an optimal Cartesian (ℓ, c) A^2-code $(\mathcal{S}, \mathcal{M}, \mathcal{E}_\mathcal{R}, \mathcal{E}_T)$ with uniform probability distributions on S and $E_T \circ E_R$ respectively such that $|S| = t$, $|AT| = |M|/|S| = \ell$, $|Split(g, s)| = c$ for all verification functions g determined by $e_R \in E_R$ and for all $s \in S$.

Proof: We construct an optimal Cartesian (ℓ, c) A^2-code from a $(t, \ell, c, 1)$-GOB design $(\mathcal{V}, \mathcal{G}, \mathcal{B})$ as follows. Each source state $s_i \in S$ corresponds to a group $G_i \in \mathcal{G}$, each message $(s_i, a_j) \in M$ corresponds to a point $p_{ij} \in G_i = \{p_{ij} : 1 \leq j \leq \ell\}$, each key of the receiver corresponds to a block $B \in \mathcal{B}$, and each key of the transmitter corresponds to a block $B' \in \mathcal{B}'$ of the associated TD(t, ℓ) $(X, \mathcal{G}, \mathcal{B}')$. Therefore, $S = \{s_1, \ldots, s_t\}$, $M = \mathcal{V}$, $E_T = \mathcal{B}'$, and $E_R = \mathcal{B}$. For any source state $s_i \in S$, the transmitter uses his key B' to compute its authentication tag $a_j \in AT$ so that (s_i, a_j) is the unique common element of B' and G_i. A key B of the receiver accepts a message $(s_i, a_j) \in M$ if and only if $p_{ij} \in B$.

To prove the optimality of this Cartesian A^2-code, we need to show that the equality of each bound in Proposition 2.2 and Corollary 2.3 is met.

$|E_T|$: $|E_T| = |\mathcal{B}'| = \ell^2$.

$|E_R|$: $|E_R| = |\mathcal{B}| = \frac{\ell^2(\ell-1)}{c^2(c-1)}$.

$|E_T \circ E_R|$: There are exactly $q_2 = \frac{\ell-1}{c-1}$ blocks of $\mathcal{B}$ containing any two elements in different groups. Therefore, each block of $\mathcal{B}'$ corresponds to $\frac{\ell-1}{c-1}$ blocks of $\mathcal{B}$, which implies that $|E_T \circ E_R| = \frac{\ell^2(\ell-1)}{(c-1)}$.

Assume that the probability distributions over S and $E_T \circ E_R$ are all uniform. For given $m \in M$, $e_R \in E_R$, and $e_T \in E_T$, define $E_T(m) = \{e_T \in E_T : e_T \text{ can generate } m \in M\}$, $E_R(m) = \{e_R \in E_R : e_R \text{ accepts } m \in M\}$, $E_T(e_R) = \{e_T \in E_T : (e_T, e_R) \in E_T \circ E_R\}$, and $E_R(e_T) = \{e_R \in E_R : (e_T, e_R) \in E_T \circ E_R\}$, respectively. Then we know that the probability distributions over E_T, E_R, $E_T(s,a)$, $E_R(s,a)$, $E_T(e_R)$ and $E_R(e_T)$ are also all uniform.

P_I : For any $(s,a) \in M$, $\Pr[R \text{ accepts } (s,a)] = \frac{|E_R(s,a)|}{|E_R|} = \frac{r}{|\mathcal{B}|} = \frac{\ell(\ell-1)/(c(c-1))}{\ell^2(\ell-1)/(c^2(c-1))} = \frac{c}{\ell}$. Therefore, $P_I = \max_{(s,a)\in M} \Pr[R \text{ accepts } (s,a)] = \frac{c}{\ell}$.

P_S : For $s, s' \in S$, $a, a' \in AT$ with $s \neq s'$, $\Pr[R \text{ accepts } (s',a') \mid T \text{ sent } (s,a)] = \frac{|E_R(s,a) \cap E_R(s',a')|}{|E_R(s,a)|} = \frac{q_2}{r} = \frac{(\ell-1)/(c-1)}{\ell(\ell-1)/(c(c-1))} = \frac{c}{\ell}$, and thus $P_S = \sum_{(s,a)\in M} \Pr[\mathcal{M} = (s,a)]$ $\max_{s'\neq s} \max_{a'\in A} \Pr[R \text{ accepts } (s',a') \mid T \text{ sent } (s,a)] = \frac{c}{\ell}$.

P_T : For $s, s' \in S$, $a \in AT$ with $s \neq s'$, $a \neq e_T(s)$, $\Pr[R \text{ accepts } (s,a) \text{ and } a \neq e_T(s) \mid T \text{ has } e_T] = \frac{|E_R(s,e_T(s)) \cap E_R(s',e_T(s')) \cap E_R(s,a)|}{|E_R(e_T)|}$. Since $|E_R(s', e_T(s')) \cap E_R(s, e_T(s)) \cap E_R(s,a)| = \lambda = 1$, and $|E_R(e_T)| = q_2$, we know that $\Pr[R \text{ accepts } (s,a) \text{ and } a \neq e_T(s) \mid T \text{ has } e_T] = \frac{1}{q_2}$, and thus $P_T = \max_{e_T \in E_T} \max_{(s,a)\in M} \Pr[R \text{ accepts } (s,a)$ and $a \neq e_T(s) \mid T \text{ has } e_T] = \frac{1}{q_2} = \frac{c-1}{\ell-1}$.

P_{R_0}, P_{R_1} : For any $e_R \in E_R = \mathcal{B}$, $|E_T(e_R)| = c^2$, $|E_T(e_R) \cap E_T(s,a)| = c$ if $(s,a) \in \mathcal{V} = M$, and $|E_T(e_R) \cap E_T(s,a) \cap E_T(s',a')| = 1$ if $(s,a), (s',a') \in \mathcal{V} = M$ with $s \neq s'$. Therefore $\Pr[T \text{ can generate } (s,a) \mid R \text{ has } e_R] = \frac{|E_T(s,a) \cap E_T(e_R)|}{|E_T(e_R)|} = \frac{c}{c^2} = \frac{1}{c}$, and for $(s',a') \in \mathcal{V} = M$ with $s \neq s'$, $\Pr[T \text{ can generate } (s',a') \mid R \text{ has } e_R \text{ and } T \text{ sent } (s,a)] = \frac{|E_T(s',a') \cap E_T(s,a) \cap E_T(e_R)|}{|E_T(s,a) \cap E_T(e_R)|} = \frac{1}{c}$. Thus, $P_{R_0} = \max_{e_R \in E_R} \max_{(s,a)\in M} \Pr[T \text{ can generate } (s,a) \mid R \text{ has } e_R] = \frac{1}{c}$, and $P_{R_1} = \max_{e_R \in E_R} \sum_{(s,a)\in M} \Pr[\mathcal{M} = (s,a)] \max_{s'\neq s} \max_{a'\in AT}$ $\Pr[T \text{ can generate } (s',a') \mid R \text{ has } e_R \text{ and } T \text{ sent } (s,a)] = \frac{1}{c}$.

□

We finally note that in any optimal (ℓ, c) A^2-code $(\mathcal{S}, \mathcal{M}, \mathcal{E}_\mathcal{R}, \mathcal{E}_\mathcal{T})$, $\mathcal{E}_\mathcal{R}$ and $\mathcal{E}_\mathcal{T}$ are all uniform. This was proved by Obana and Kurosawa [8].

5 An Extended Family of Optimal A^2-Codes

Johansson [4] constructed a family of optimal A^2-codes from a projective space $PG(3, q)$. In this section, we generalize his result to obtain an extended family of optimal A^2-codes.

Let Π_i be the set of i-dimensional subspaces in a projective space $PG(3+d, q)$, $0 \leq i \leq 3+d$. So, Π_0 is the set of points, Π_1 the set of lines, Π_2 the set of planes, and Π_{2+d} the set of hyperplanes. If S is an arbitrary set of points in the projective space, then $span\langle S\rangle$ is the intersection of all subspaces containing S.

Fix a subspace Γ in Π_{1+d}. Take

$$\mathcal{V} = \Pi_0 \setminus \Gamma.$$

Take a point $x_1 \in \Pi_0 \setminus \Gamma$. Then $span\langle \Gamma, x_1\rangle$ is a hyperplane. Take another point $x_2 \in \Pi_0 \setminus span\langle \Gamma, x_1\rangle$, and let $L = \{x_1, x_2, \ldots, x_{q+1}\}$ be the line containing both x_1 and x_2. Then $L \cap \Gamma = \emptyset$ and the $q+1$ hyperplanes $P_i = span\langle \Gamma, x_i\rangle$ exhaust all points in Π_0. Denote

$$G_i = P_i \setminus \Gamma.$$

Then $G_1, G_2, \ldots, G_{q+1}$ form a partition of $\mathcal{V}$. Let $\mathcal{G} = \{G_1, G_2, \ldots, G_{q+1}\}$.

Since Γ, P_i and Π_0 contain respectively $\frac{q^{2+d}-1}{q-1}$, $\frac{q^{3+d}-1}{q-1}$ and $\frac{q^{4+d}-1}{q-1}$ points, we have

$$|G_i| = q^{d+2},$$

where $1 \leq i \leq q+1$, and

$$|\mathcal{V}| = q^{d+3} + q^{d+2}.$$

Since the intersection of Γ and any plane $P \in \Pi_2$ is a subspace, $dim(\Gamma \cap P) = 0$ if and only if $|P \cap \Gamma| = 1$. Let

$$\mathcal{B} = \{P \in \Pi_2 : \ |\Gamma \cap P| = 1\}$$

be the collection of blocks. Any block is a plane intersecting Γ in one point. Take a block B, and denote $B \cap \Gamma = \{w\}$. Any P_i, $1 \leq i \leq q+1$, intersects B in a line which contains w. Since $w \notin G_i$, we have

$$|B \cap G_i| = q$$

for $i = 1, 2, \ldots, q+1$. We can show that $(\mathcal{V}, \mathcal{G}, \mathcal{B})$ is a (t, ℓ, c, λ)-GOB design with $t = q+1$, $\ell = q^{d+2}$, $c = q$ and $\lambda = 1$. We verify conditions for a GOB design below.

Let any two points in the same G_i, $i = 1, 2, \ldots, q+1$, be 1st associates, and any two points in distinct groups G_i and G_j, $i, j = 1, 2, \ldots, q+1$, be 2nd associates. Then in this way we naturally obtain a group divisible association scheme. Suppose that $y, z \in G_i$ for some i, $1 \leq i \leq q+1$. Let $L(y, z)$ be the line containing both y and z. Suppose that B is a block containing both y and z. Then B must contain $L(y, z)$. For any G_j, $i \neq j$, $1 \leq j \leq q+1$, since $|B \cap G_j| = q$, we have that $B \cap P_j$ is a line. For any $x \in G_j$, $span\langle x, L(y, z)\rangle$ is a plane intersecting Γ in one point; otherwise, x, y, z would have to be

in the same group which is impossible. Hence $span\langle x, L(y,z)\rangle$ is a block in $\mathcal{B}$. There are exactly $|G_j|/q = q^{d+1}$ blocks containing both y and z. Suppose $y \in G_i$ and $x \in G_j$ for some distinct i and j, $1 \le i, j \le q+1$. For any $z \in G_i$, $span\langle x, L(y,z)\rangle$ is a block in $\mathcal{B}$. Since there are $|G_i - \{y\}|/(q-1)$ lines $L(y,z)$, $z \in G_i$, in P_i containing y, there are $\frac{q^{d+2}-1}{q-1}$ blocks containing both $y \in G_i$ and $x \in G_j$. So,

$$\lambda_1 = q^{d+1}, \quad \lambda_2 = \frac{q^{d+2}-1}{q-1},$$

and we verified that $(\mathcal{V}, \mathcal{G}, \mathcal{B})$ is a GD design with λ_1 and λ_2 described above.

Take any distinct groups G_i, G_j, G_k and any fixed points x, y such that $x \in G_i$ and $y \in G_j$. Denote $L(x,y) \cap P_k = \{z\}$. If $z \in \Gamma$, then x and y would have to be in the same group, which is impossible. Since $z \notin \Gamma$, we have $z \in G_k$. For any block B containing both $x \in G_i$ and $y \in G_j$, B contains the line $L(x,y)$ and therefore the point $z \in G_k$ too. This verifies condition (2).

Take any fixed group $G_i \in \mathcal{G}$ and any fixed point $x \in \mathcal{V} \setminus G_i$. For any two distinct points y and z in G_i, $x \notin L(y,z)$ since $x \notin P_i$. There is a unique plane P containing all x, y and z. P intersects Γ in one point; otherwise x would have to be in G_i. Therefore, P is the unique block in $\mathcal{B}$ containing $x \in \mathcal{V} \setminus G_i$ and the two given distinct points $y \in G_i$ and $z \in G_i$. We have $\lambda = 1$ and condition (3) is verified.

We have proved that $(\mathcal{V}, \mathcal{G}, \mathcal{B})$ is a (t, ℓ, c, λ)-GOB design with $t = q+1$, $\ell = q^{d+2}$, $c = q$ and $\lambda = 1$. The other parameters are $|\mathcal{V}| = q^{d+3} + q^{d+2}$, $|\mathcal{B}| = \frac{q^{2d+2}(q^{d+2}-1)}{q-1}$, $\lambda_1 = q^{d+1}$ and $\lambda_2 = \frac{q^{d+2}-1}{q-1}$.

Theorem 5.1 There exists a $(q+1, q^{d+2}, q, 1)$-GOB design for any prime power q and any non-negative integer d.

According to Thereom 4.3, we in fact constructed a family of optimal A^2-codes.

Theorem 5.2 There exists an optimal Cartesian (q^{d+2}, q) A^2-code $(\mathcal{S}, \mathcal{M}, \mathcal{E}_{\mathcal{R}}, \mathcal{E}_{\mathcal{T}})$ for any prime power q and any non-negative integer d with uniform probability distributions on S and $E_T \circ E_R$ respectively such that $|S| = q+1$, $|AT| = |M|/|S| = q^{d+2}$, $|Split(g,s)| = q$ for all verification functions g determined by $e_R \in E_R$ and for all $s \in S$.

We wish to remark that when $d = 0$, we obtain the well-known Johansson's family of optimal A^2-codes [4].

6 Conclusions

In this paper, we revisited the known combinatorial characterization of optimal authentication codes with arbitration in [7, 8, 10, 18]. We introduced the notion of a GOB design

and then investigated its structure. We used GOB designs to re-characterize optimal authentication codes with arbitration, which is much easier to be understood than the previous ones. This new characterization enabled us to construct a new family of optimal authentication codes with arbitration from finite geometries.

Acknowledgments: The research of the first author is supported by National Natural Science Foundation of China under Grant No. 10471127 and Zhejiang Provincial Natural Science Foundation of China under Grant No. R604001.

References

[1] E. F. Brickell and D. R. Stinson, *Authentication codes with multiple arbiters*, in: Proc. EUROCRPT'88, Lecture Notes in Comput. Sci. **330** (1988), 51–55.

[2] E. N. Gilbert, F. J. MacWilliams and N. J. A. Sloane, *Codes which detect deception*, Bell Syst. Tech. J. **53** (1974), 405–424.

[3] M. Jimbo and R. Fuji-Hara, *Optimal authentication systems and combinatorial designs*, IEEE Trans. Inform. Theory **36** (1990), 54–62.

[4] T. Johansson, *Lower bounds on the probability of deception in authentication with arbitration*, IEEE Trans. Inform. Theory **40** (1994), 1573–1585.

[5] K. Kurosawa and S. Obana, *Combinatorial bounds on authentication codes with arbitration*, Des. Codes Cryptogr. **22** (2001), 265–281.

[6] J. L. Massey, *Cryptography – a selective survey*, in: Digital Communications, North-Holland, 1986, 3–21.

[7] S. Obana and K. Kurosawa, *A^2-code = affine resolvable + BIBD*, in: ICICS'97, Lecture Notes in Comput. Sci. **1334** (1997), 130–143.

[8] S. Obana and K. Kurosawa, *Combinatorial classification of optimal authentication codes with arbitration*, Des. Codes Cryptogr. **20** (2000), 281–305.

[9] D. Pei and Y. Li, *Optimal authentication codes with arbitration* (in Chinese), Acta Math. Appl. Sin. 25 (2002), 88–100.

[10] D. Pei, Y. Li, Y. Wang and R. Safavi-Naini, *Characterization of optimal authentication codes with arbitration*, in: ACISP'99, Lecture Notes in Comput. Sci. **1587** (1999), 303–313.

[11] C. R. Rao, *Factorial experiments derivable from combinatorial arragements of arrays*, J. Roy. Soc., Suppl. **9** (1947), 128–139.

[12] R. S. Safavi-Naini and J. R. Seberry, *Error-correcting codes for authentication and subliminal channels*, IEEE Trans. Inform. Theory **37** (1991), 13–17.

[13] G. J. Simmons, *Authentication theory/coding theory*, in: CRYPTO'84, Lecture Notes in Comput. Sci. **196** (1985), 411–431.

[14] G. J. Simmons, *Message authentication with arbitration of transmitter/receiver disputes*, in: EUROCRYPT'87, Lecture Notes in Comput. Sci. **304** (1988), 151–165.

[15] G. J. Simmons, *A Cartesian product construction for unconditionally secure authentication codes that permit arbitration*, J. Cryptology **2** (1990), 77–104.

[16] D. R. Stinson, *The combinatorics of authentication and secrecy codes*, J. Cryptology **2** (1990), 23–49.

[17] Y. Wang, *Information-theoretic lower bounds for authentication codes with arbitration* (in Chinese), in: CHINACRYPT'98, Science Press, 1998, 99–104.

[18] Y. Wang, R. Safavi-Naini and D. Pei, *Combinatorial characterization of ℓ-optimal authentication codes with arbitration*, J. Combin. Math. Combin. Comput. **37** (2001), 205–224.